UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/055,572	10/19/2001	Tom L. Nguyen	42390P12549	6116

8791 7590 01/23/2007	EXAMINER	
BLAKELY SOKOLOFF TAYLOR & ZAFMAN	BESROUR, SAOUSSEN	
12400 WILSHIRE BOULEVARD		
SEVENTH FLOOR	ART UNIT	PAPER NUMBER
LOS ANGELES, CA 90025-1030	2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
	10/055,572	NGUYEN ET AL.
Office Action Summary	Examiner	Art Unit	
	Saoussen Besrour	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 6-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 3, 4 and 6-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to amendment filed 11/2/2006.   Claims 1, 2, 3, 4, 6, 7,

8, 9, 10, 11, 12, 13, 16, 17 and 19 were amended. Claims 5 and 20-30 were cancelled.

Claims 1, 2, 3, 4 and 6-19 are pending.

Continued Examination Under 37 CFR 1.114

3.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

11/2/2006 has been entered.

Claim Objections

4.   **Claims 1, 7, 8, 9,10 and 19** are objected to because of the following

informalities:

As per **claims 7, 8 and 9**: replace "the current data" with "current data."

As per **claims 1, 9, 10 and 19**: Use of the word "if" generates a conditional

statement, replace "if" with "when". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

5.   **Claim 10** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

Claim 10 recites the limitation "the current content" in line 7 of the claim. There is

insufficient antecedent basis for this limitation in the claim. For the purpose of this

examination examiner presumes that "the current content" is the content stored in the

first device.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   **Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18 and 19** are rejected

under 35 U.S.C. 103(a) as being unpatentable over Noll (US 6,185,696) in view of

Chaiken et al. (US 6,757,838).

As per **claim 1**, Noll discloses: a first non-volatile data storage device, configured

as one or more storage regions, to store one or more bytes of CMOS BIOS data (Fig. 1

#22, Column 2, Lines 40-43); another, second non-volatile data storage device to store

a mirror image of the CMOS BIOS data (Fig.1 #30); a program store to store one or

more processor-readable instructions to ascertain the validity of the CMOS BIOS data

stored in the first non-volatile storage device and if invalid to replace the SMOS BIOS

data in the first non-volatile storage device with the stored mirror image of the data

(Column 6, Lines 23-40); and a processing unit coupled to the first and second non-

volatile data storage devices and program store, to read and process the one or more

instructions in the program code (Fig. 1 #12). Noll does not explicitly teach wherein the

first non-volatile data storage device lacks hardware security such that some of the

CMOS BIOS regions are modifiable by an application program on the system; and

wherein the second non-volatile storage device to store the mirror data in a location that

cannot be modified without system authorization. However Chaiken et al. discloses:

wherein the first non-volatile data storage device lacks hardware security such that

some of the CMOS BIOS regions are modifiable by an application program on the

system (Column 9, Lines 63-Column 10, Lines 4 new hardware, and Column 2, Lines

59-Column 3, Lines 4); and wherein the second non-volatile storage device to store the

mirror data in a location that cannot be modified without system authorization (Column

2, Lines 59-Column 3, Lines 4). Therefore, it would have been obvious to one with

ordinary skill in the art at the time the invention was made to use the teaching of

Chaiken et al. in conjunction with the teachings of Noll for the benefit of securing the

backup BIOS from alteration such as overwriting or flashing (Column 2, Lines 67).

As per **claim 10**, Noll discloses: reading current CMOS BIOS content stored in a

first non-volatile storage device of a system (Fig. 1#22); reading from a valid image of

the CMOS BIOS content, that us stored in a further second non-volatile storage device

(Fig. 1 #30); determining if the current content has been modified without authorization (Column 6, Lines 23-40) and replacing the stored current content with said stored valid image of the content if the current content is determined to have been modified without authorization (Column 6, Lines 23-40). Noll does not explicitly teach wherein the first device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system. However, Chaiken et al. discloses: wherein the first device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system (Column 9, Lines 63-Column 10, Lines 4 new hardware, and Column 2, Lines 59-Column 3, Lines 4). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teaching of Chaiken et al. in conjunction with the teachings of Noll for the benefit of securing the backup BIOS from alterations such as overwriting or flashing (Column 2, Lines 67).

As per **claim 17**, Noll discloses: arranging a first non-volatile storage device of a computer system into one or more storage regions to store CMOS BIOS data (Fig. 1 #22 Column 2, Lines 40-43); generating an integrity metric corresponding to valid CMOS BIOS content stored in a first region of the first non-volatile storage device (Column 5, Lines 29-33). Noll does not explicitly teach: wherein the first device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system; and storing the integrity metric in another, second non-volatile storage device of the computer system to later determine if the content in

the first region has been modified without authorization. However, Chaiken et al. discloses: wherein the first device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system (Column 9, Lines 63-Column 10, Lines 4 new hardware, and Column 2, Lines 59-Column 3, Lines 4); and storing the integrity metric in another, second non-volatile storage device of the computer system to later determine if the content in the first region has been modified without authorization (Column 8, Lines 40-45). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teaching of Chaiken et al. in conjunction with the teachings of Noll for the benefit of securing the backup BIOS from alterations such as overwriting or flashing (Column 2, Lines 67).

As per **claim 2**, rejected as applied to claim 1. Furthermore, Noll discloses: to process the instructions in the program store as part of a start-up procedure (Column 4, Lines 60-Column 5, Lines 50).

As per **claim 3**, rejected as applied to claim 1. Furthermore, Chaiken discloses: wherein the program store is inside the second non-volatile data storage device (Column 8, Lines 39-47).

As per **claim 4**, rejected as applied to claim 1. Furthermore, Chaiken discloses: wherein the processor-readable instructions in the program store ascertain the validity of the data stored in the first non-volatile storage device on a region-by-region basis (Fig.3B, 304A-304N)

As per **claim 6**, rejected as applied to claim 4. Furthermore, Chaiken discloses: employing a system interface to perform modifications to the data stored in said second non-volatile data storage device (Column 10, Lines 5-10).

As per **claim 7**, rejected as applied to claim 1. Furthermore, Chaiken discloses: determining if the current data in the first non-volatile storage device is different than the stored image of the data (Column 8, Lines 40-46).

As per **claim 8**, rejected as applied to claim 1. Furthermore, Chaiken discloses: determining if an integrity metric corresponding to the current data in the first non-volatile storage device is different than the same integrity metric corresponding to the stored image of the data (checksum, CRC, Column 8, Lines 40-46).

As per **claim 9**, rejected as applied to claim 1. Furthermore, Chaiken discloses: generating a copy of the current data in the first non-volatile memory device if an authorized application modifies the current data and storing the copy as a valid image of the current data (Column 9, Lines 63- Column 10, Lines 10).

As per **claim 11**, rejected as applied to claim 10. Furthermore, Chaiken discloses: comparing the read valid image to the current content to determine if the current content has been modified (Column 8, Lines 40-46).

As per **claim 12**, rejected as applied to claim 10. Furthermore, Chaiken discloses: comparing a previously stored checksum, corresponding to the valid image of the content, and a checksum corresponding to the current content (Column 8, Lined 40-46).

As per **claim 13**, rejected as applied to claim 10. Furthermore, Chaiken

discloses: comparing a previously stored cyclic redundancy check value, corresponding

to the valid image of the content, and a cyclic redundancy check value corresponding to

the current content (Column 8, Lined 40-46).

As per **claim 15**, rejected as applied to claim 10. Furthermore, Noll discloses:

storing a valid image of the current content for later use (Fig. 1 #30, Column 5, Lines

46-50).

As per **claim 16**, rejected as applied to claim 10. Furthermore, Noll discloses:

wherein reading the current content from the first non-volatile storage device is part of a

start up procedure of the system (Column 4, Lines 60-50).

As per **claim 18**, rejected as applied to claim 17. Furthermore, Noll discloses:

comparing a previously stored integrity metric, corresponding to an earlier version of the

content stored in the first region, to a newly calculated integrity metric corresponding to

the current content stored in the first region to determine if an unauthorized modification

has occurred (Column 5, Lines 29-33).

As per **claim 19**, rejected as applied to claim 17. Furthermore, Noll discloses

replacing the content of the first region with an earlier version of the content therein if it

is determined that there was unauthorized modification (Column 6, Lines 23-30).

7.   **Claim 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll

(US 6,185,696) in view of Chaiken et al. (US 6,757,838) in further view of Huh et al.

(U.S. Patent No. 6,584,559).

As per **claims 14**, rejected as applied to claim 10. The combined references Noll et al. and Chaiken et al. substantially teach reading current CMOS BIOS content stored in a first non-volatile storage device of a system, wherein the first device lacks hardware security such that the CMOS BIOS content is modifiable by an application program in the system; reading from a valid image of the CMOS BIOS content, that is stored in a second further non-volatile storage device; determining if the current content has been modified without authorization; and replacing the stored current content with said stored valid image of the content if the current content is determined to have been modified without authorization.

The combined teachings of Noll et al. and Chaiken et al. do not explicitly teach comparing a previously stored bit mask, corresponding to the valid image of the content, and a bit mask corresponding to the current content. However, Huh et al. discloses comparing a previously stored bit mask, corresponding to the valid image of the content, and a bit mask corresponding to the current content (Column 4, Lines 11-13).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Huh et al. in conjunction with the combined teachings of Noll et al. and Chaiken et al. for the benefit of validating the firmware (Column 1, Lines 63-66).

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to
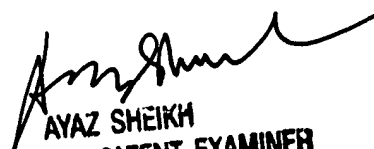
applicant's disclosure.

Mermestein (US 6,715,106)

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Saoussen Besrour whose telephone number is 571-272-

6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

      If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

      Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
January 17, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100